South Carolina Department of Insurance
1201 Main Street, Suite 1000
Columbia, SC 29201

Mailing Address
P.O. Box 100105
Columbia, SC 29202

BULLETIN NUMBER 2020-04

TO: All Licensees of the South Carolina Department of Insurance, including Guaranty Fund Associations, Surplus LineInsurers and Other Persons Registered or Authorized to Operate Pursuant to the Insurance Laws of this State

FROM: Raymond G. Farmer Director of Insurance

SUBJECT: Guidance for Licensees Regarding Third-Party Service Providers - South Carolina Insurance Data Security Act, 2018 S.C. Act No. 171

DATE: April 17, 2020

I. OVERVIEW

This is the fourth in the series of bulletins regarding the implementation of the South Carolina Insurance Data Security Act (SCIDSA). As you are aware, the SCIDSA requires licensees that are not exempt from the information security program requirements of the SCIDSA to establish additional oversight of third-party service providers on or before July 1, 2020. Non-exempt licensees must exercise due diligence in selecting third-party service providers and ensure selected third-party service providers implement appropriate administrative, technical and physical measures to protect and secure the information system and nonpublic information (NPI) that are accessible to, or held by, the third-party service provider. *See* S.C. Code Ann. Section 38-99-20(F) (2018). Third-party service providers have been responsible for most of the cyber event notifications the South Carolina Department of Insurance (Department) has received to date.

The information provided in this bulletin and our website does not, and is not intended to, constitute legal advice. Instead, the purpose of this information is to outline issues that should be considered when reviewing the use of third-party service providers as part of a licensee's broader information security program. Licensees should ultimately be guided by their risk assessment and implement procedures commensurate with the size and complexity of their business. It is recommended that you contact your attorney for legal advice on issues related to the implementation of your information security program.

II. THIRD-PARTY SERVICE PROVIDERS (TPSP)

A third-party service provider is defined as *a person not otherwise defined as a licensee that contracts with a licensee to maintain, process, store or otherwise is permitted access to nonpublic information through its provision of services to the licensee*. *See* S.C. Code Ann. Section 38-99-10 (2018).

This may include business arrangements between a licensee and another person (by contract or otherwise) that involve outsourced products and services, use of independent consultants, networking arrangements, merchant paying processing services, services provided by affiliates and subsidiaries, joint ventures, and other arrangements where the TPSP has an ongoing relationship with the licensee

and access to the licensee's NPI. Third-party relationships do not include customer or policyholder relationships.

The SCIDSA requires licensees to implement and exercise effective risk management in their third-party relationships. A licensee's use of TPSPs does not diminish the licensee's responsibility through its board of directors or senior management to ensure that the TPSP is effectively safeguarding NPI in accordance with the SCIDSA and other applicable law.

III. REGULATORY REVIEWS OF THIRD-PARTY RELATIONSHIPS

The Department expects licensee management to engage in a robust analytical process to identify, measure, monitor, and control the risks associated with third-party relationships and to avoid excessive risk taking that may threaten a licensee's operational safety and soundness. A licensee's failure to have an effective third-party risk management process that is commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including its use of TPSPs, and the sensitivity of the NPI used by the licensee may constitute an unsound or hazardous condition.

Licensees should advise TPSPs that the performance of activities by external parties for the licensee may be subject to Department examination oversight. The Department has jurisdiction over all situations in which a licensee arranges, by contract or otherwise, for the performance of any applicable functions of its operations.

The Department will pursue appropriate corrective action against the licensee, including enforcement action, to address violations of applicable laws and regulations or illegal or unfair practices by the licensee or its third-party. The Department has the authority to assess a licensee the costs of the examination.

IV. QUESTIONS

This bulletin and additional reference materials available on our website (www.doi.sc.gov/cyber), including checklists and links to resources about third-party service provider programs are based upon guidance provided by federal regulatory agencies and information security accrediting organizations. Questions regarding this bulletin should be directed to Melissa Manning at mmanning@doi.sc.gov.